Funzionalità dei Malware

Identificazione del Tipo di Malware

Il malware sembra essere progettato per installare un hook alla coda degli eventi di Windows (specificamente legato al mouse) e successivamente copiare un file in una cartella di avvio del sistema per ottenere persistenza. Questo comportamento è tipico di **malware di tipo keylogger** o di **backdoor** che cerca di monitorare le attività dell'utente e/o di ottenere persistenza nel sistema infetto.

Chiamate di Funzione Principali e Descrizione

1. **SetWindowsHook()**:
    - **Descrizione**: Questa chiamata di funzione è utilizzata per installare un hook, ovvero un filtro che intercetta gli eventi della coda di messaggi di Windows. Nel caso specifico, il parametro WH_MOUSE indica che l'hook è associato agli eventi del mouse. Questo è spesso utilizzato dai keylogger per tracciare i movimenti del mouse o per catturare gli eventi di clic.
2. **CopyFile()**:
    - **Descrizione**: Questa chiamata di funzione viene utilizzata per copiare un file da una posizione a un'altra. Nel contesto del codice, sembra che il malware stia copiando sé stesso o un file associato in una directory specifica, indicata da EDI (che nel commento viene descritto come il percorso della cartella di avvio del sistema).

Metodo di Persistenza

Il malware ottiene la persistenza copiando un file nella cartella di avvio del sistema operativo, come indicato dal commento EDI = «path to startup_folder_system». Copiando il proprio file in questa cartella, il malware si assicura di essere eseguito automaticamente ogni volta che il sistema viene avviato.

Analisi a Basso Livello delle Istruzioni

- **push eax, push ebx, push ecx**: Queste istruzioni salvano i registri eax, ebx, e ecx sullo stack per preservarne i valori prima di effettuare chiamate di funzione. Questo è un pattern comune prima di eseguire chiamate di sistema in assembly.
- **push WH_Mouse**: Inserisce il valore WH_MOUSE nello stack, che sarà passato come parametro alla funzione SetWindowsHook() per indicare il tipo di hook da installare.
- **call SetWindowsHook()**: Effettua la chiamata alla funzione SetWindowsHook() con i parametri precedentemente inseriti nello stack, installando così l'hook per il mouse.
- **XOR ECX,ECX**: Azzera il registro ECX impostandolo a zero (poiché XOR di un registro con sé stesso restituisce sempre zero). Questo potrebbe essere utilizzato per preparare il registro per un'operazione successiva.
- **mov ecx, [EDI]**: Carica nel registro ECX il valore contenuto all'indirizzo puntato da EDI, che corrisponde al percorso della cartella di avvio del sistema.
- **mov edx, [ESI]**: Carica nel registro EDX il valore contenuto all'indirizzo puntato da ESI, che corrisponde al percorso del file malware che deve essere copiato.

- **push ecx**: Inserisce il valore di ECX nello stack, che con molta probabilità rappresenta il percorso di destinazione per il file da copiare.
- **push edx**: Inserisce il valore di EDX nello stack, che rappresenta il percorso del file da copiare.
- **call CopyFile()**: Effettua la chiamata alla funzione CopyFile() per copiare il file dal percorso sorgente (nel registro EDX) al percorso di destinazione (nel registro ECX).

Conclusione

Questo codice assembly rappresenta un malware che:

1. Installa un hook per monitorare eventi del mouse tramite la funzione SetWindowsHook().
2. Ottiene persistenza copiando un file (potenzialmente il malware stesso) nella cartella di avvio del sistema operativo, assicurandosi che venga eseguito automaticamente all'avvio del sistema.